Techniques for EM Fault Injection: Equipments and Experimental Results

Philippe Maurine

▶ **To cite this version:**

Philippe Maurine. Techniques for EM Fault Injection: Equipments and Experimental Results. FDTC'2012: Fault Diagnosis and Tolerance in Cryptography, Sep 2012, Lewen, Belgium. pp.003-004. lirmm-00761778

HAL Id: lirmm-00761778
https://hal-lirmm.ccsd.cnrs.fr/lirmm-00761778

Submitted on 6 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Techniques for EM fault Injection: Equipments and Experimental Results

Philippe Maurine
LIRMM, University UMR 5506
Montpellier, France
leader of the ANR 2010-SEGI-012-01 project (EMAISeCi)
pmaurine@lirmm.fr

***Keywords*-EM Fault Injection techniques; Equipments**

These last years, the advances realized by technologists and circuit designers were particularly important. Alongside these advances, the demand of secure objects tended to broaden from smartcard towards high performance integrated products. These Systems on Chip that will have ultimately to offer robustness guarantees against physical attacks, have characteristics radically different from those of smartcards. Indeed, the comparison of SoC with smartcards highlights that SoC:

- operate at several hundreds of MHz against few tens of MHz for smartcards,
- feature several millions of CMOS gates against roughly one hundred thousand for modern smartcards,
- are designed with advanced CMOS technologies (45nm, 32nm) on a bulk or a Silicon on insulator substrate, while smartcards are currently designed with the 90nm process,
- have a large number of IO and supply/ground pins and are often encapsulated in a ball grid array package.

These observations raise questions about the vulnerabilities of tomorrow's embedded systems against physical attacks. Will an adversary be able to analyze the power consumption of such systems? Will he be able to inject transient faults and exploit them in such systems? If the issue of physical vulnerabilities of SoC remains, as designers of secure circuits, we can only wonder about the means that could be used by adversaries in order to inject transient faults into a SoC running at several hundreds of MHz encapsulated in a bga package. Considering that adversaries can access only the front side of such systems, the above questions lead to consider the ElectroMagnetic waves as the main medium for inject faults as proposed in the seminal works [6], [7]. Within this context, two EM platforms for injecting faults into circuits will be described during the presentation.

The first of these plateforms is an harmonic injection platform depicted in Figure 1. The latter has been developed in order to be able to disturb some analogue blocks as on-chip clock generators [5] or some TRNGs [1]. The challenges related to this kind of injection will be discussed before presenting some experimental results. The second platform, shown in Figure 2, is dedicated to the injection of EM pulses.

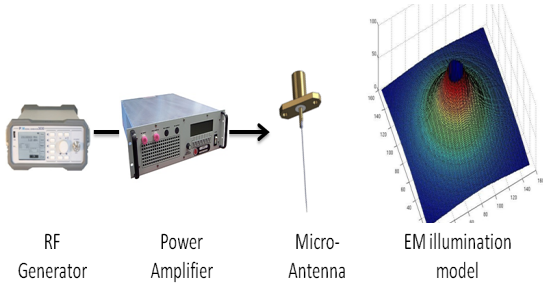

Figure 1. 'Principle of the EM Harmonic Injection platform'

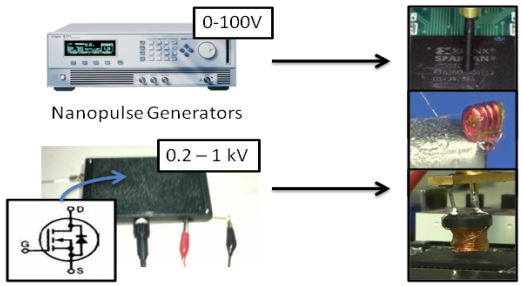

Figure 2. 'Principle of the EM pulse Injection platform'

This type of injection platform has been developped to inject transient faults within sensitive operations performed by some cryptomodules or any processing elements [3]. Two types of platforms can be designed. A medium voltage platform (0-100V) centered on a pulse generator available on the market. A high voltage platform (50V-1kV) based on an homemade pulse generator such as the one proposed in [2]. Experimental results obtained when applying the Piret-Quisquater attack [4] will be analyzed to identify one of the electrical behaviors that could explain the occurence of transient faults.

Finally, we will show that EM backside injection (case of flip chip bga packages) has little or no interest. Indeed, a new fault injection technique, called Forward Body Biaising Injection (FBBI), must be preferred to EM injection to produce transient faults, especially when LASER shots are detected by the target. The equipement required to apply a FBBI is low cost and really similar to the one used to

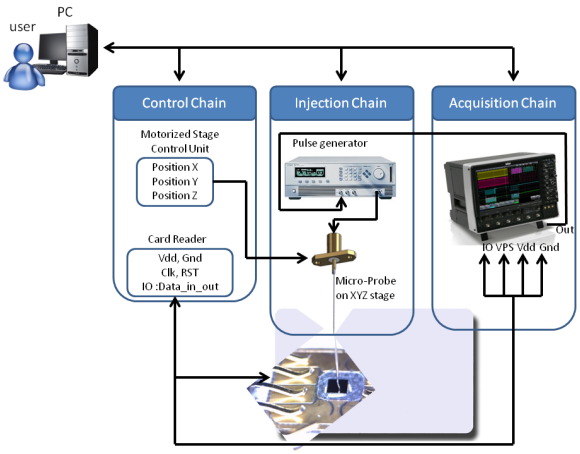

Figure 3. 'Principle of the FBBI platform'

produce an EM pulse. It is shown in 3. The main difference is the replacement of the coil producing the magnetic field by a thin tungsten rod in order to directly establish an electrical contact with the substrate. With such a direct contact (instead of a magnetic coupling), the fault can be produced with a low amplitude pulse generator. Additionally, the spatial resolution is expected to be better than with an EM pulse. The two electrical behaviors underlying this simple technique will be described before giving some experimental results obtained on a CRT based RSA, running on a secure device featuring a modular arithmetic co-processor.

REFERENCES

[1] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *COSADE*, pages 151–166, 2012.

[2] Drew Campbell, Jason Harper, Vinodhkumar Natham, Funian Xiao, and Raji Sundararajan. A compact high voltage nanosecond pulse generator. In *ESA Annual Meeting on Electrostatics*, pages 1–12, 2008.

[3] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, P. Orsatelli, Philippe Maurine, and Assia Tria. Injection of transient faults using electromagnetic pulses -practical results on a cryptographic system-. *IACR Cryptology ePrint Archive*, 2012:123, 2012.

[4] Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In *CHES*, pages 77–88, 2003.

[5] François Poucheret, Karim Tobich, Mathieu Lisart, Laurent Chusseau, Bruno Robisson, and Philippe Maurine. Local and direct em injection of power into cmos integrated circuits. In *FDTC*, pages 100–104, 2011.

[6] David Samyde, Sergei P. Skorobogatov, Ross J. Anderson, and Jean-Jacques Quisquater. On a new way to read data from memory. In *IEEE Security in Storage Workshop*, pages 65–69, 2002.

[7] Jörn-Marc Schmidt and Michael Hutter. Optical and EM fault-attacks on CRT-based RSA: Concrete results. In Johannes Wolkerstorfer Karl C. Posch, editor, *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61–67. Verlag der Technischen Universität Graz, 2007.